

**MULTI STATE INFORMATION SHARING AND INFORMATION ANALYSIS CENTER -
CYBER INFORMATION BULLETIN**

DATE ISSUED:

September 1, 2005

SUBJECT:

Fraudulent Websites for Hurricane Katrina Victims

OVERVIEW:

We have received information indicating that Internet domain names are being created that could be used to lure unwary users into visiting potentially malicious web sites.

BULLETIN:

Relief and charity efforts for the victims of Hurricane Katrina began immediately after the hurricane devastated the Gulf Coast area. Shortly thereafter, web sites began to appear which were designed to defraud unsuspecting users. Some of the activities include soliciting donations for seemingly charitable purposes, attempting to collect personal information through phishing scams and also spreading malware to unsuspecting users. Over the past few days, domain names that redirect users to malicious web sites have appeared online, in addition to email scams requesting donations for those impacted by the hurricane. While some of these sites and messages may be legitimate, many are not. At the time of this bulletin, please be aware that the following domains are reported to be suspicious:

- katrinahelp.com
- katrinacleanup.com
- katrinarelief.com.

Please note that this is not an exhaustive list and additional domains may continue to appear. In addition to fraudulent web sites, opportunists may use this event as a vehicle for other types of online attacks. For example, email messages that claim to contain attachments with photos, video, or other information about Hurricane Katrina may actually contain viruses, worms, or other malware.

RECOMMENDATIONS:

- We recommend that staff be advised to:
- Validate the relief fund or charity through a known reliable entity. Please refer to the FEMA link below for a list of reputable disaster relief resources for Hurricane Katrina.
- When a message containing a request for donations for these victims appears, do not respond unless you are certain it is a valid message.
- Avoid visiting untrusted web sites.
- Avoid opening email messages and attachments that claim to contain video, photos, or other information relating to relief solicitation for Hurricane Katrina.
- Follow standard best practices for email and web browsing security.

Refer to the FEMA link below for a list of reputable disaster relief resources for Hurricane Katrina.
<http://www.fema.gov/press/2005/katrinadonations.shtm>